# COVER SHEET FOR AMENDMENT OF POST-TRAVEL SUBMISSION

**Instructions:** Use this form as a cover sheet for any paperwork you may need to submit to the **Office of Public Records** in order to make your Privately Sponsored Post-Travel Submission complete in accordance with Rule 35. **Only complete this form if you need to submit an amendment to a post-travel filing you have already submitted.**

SUBMIT DIRECTLY TO THE **OFFICE OF PUBLIC RECORDS IN 232 HART BUILDING**

Name of Traveler: Michael K. Stransky

Employing Office/Committee: Republican Policy Committee

Private Sponsor(s) (List all): Stanford University's Hoover Institution

Travel Date(s): August 14-17, 2017

Description/Title of Attached Forms: Amended RE-2 Form; Complete list of invitees; Copy of the invitation from the sponsor; Itinerary (final version)

Purpose of Amendment (describe the reason for amending original submission): Post-travel submission must be amended with the Office of Public Records in SH-232.

10.20.17
*(Date)*

Michael K
*(Signature of Traveler)*

(Revised 1/3/2011)

# Employee Post-Travel Disclosure of Travel Expenses

Date/Time Stamp:

27712

SECRETARY OF THE SENATE

17 SEP -8 PM 2:32

**Post-Travel Filing Instructions:** Complete this form within **30 days** of returning from travel. Submit all forms to the **Office of Public Records in 232 Hart Building.**

In compliance with Rule 35.2(a) and (c), I make the following disclosures with respect to travel expenses that have been or will be reimbursed/paid for me. I also certify that I have attached:

□ The **original** *Employee Pre-Travel Authorization* (Form RE-1), **AND**
□ A copy of the *Private Sponsor Travel Certification Form* with all attachments (itinerary, invitee list, etc.)

Private Sponsor(s) (list all): Stanford University's Hoover Institution

Travel date(s): August 14-17, 2017 (added by amended correction 10.20.17)

Name of accompanying family member (if any): N/A
Relationship to Traveler: □ Spouse □ Child

IF THE COST OF LODGING DID NOT INCREASE DUE TO THE ACCOMPANYING SPOUSE OR DEPENDENT CHILD, ONLY INCLUDE LODGING COSTS IN EMPLOYEE EXPENSES. (Attach additional pages if necessary.)

**Expenses for Employee:**

| | Transportation Expenses | Lodging Expenses | Meal Expenses | Other Expenses (Amount & Description) |
|---|---|---|---|---|
| □ Good Faith Estimate<br>☒ Actual Amount | $579.29 - Flight | $450 | $182.50 | $82.63 - Ground Transportation |

**Expenses for Accompanying Spouse or Dependent Child** (if applicable):

| | Transportation Expenses | Lodging Expenses | Meal Expenses | Other Expenses (Amount & Description) |
|---|---|---|---|---|
| □ Good Faith Estimate<br>□ Actual Amount | N/A | N/A | N/A | N/A |

Provide a description of all meetings and events attended. *See* Senate Rule 35.2(c)(6). (Attach additional pages if necessary.):

See Attached Syllabus

9.8.17
*(Date)*

Michael Stransky
*(Printed name of traveler)*

Michael
*(Signature of traveler)*

TO BE COMPLETED BY SUPERVISING MEMBER/OFFICER:

I have made a determination that the expenses set out above in connections with travel described in the *Employee Pre-Travel Authorization* form, are necessary transportation, lodging, and related expenses as defined in Rule 35.

9/8/17
*(Date)*

John Barrasso
*(Signature of Supervising Senator/Officer)*

(Revised 1/3/11)

Form RE-2

Stanford University

Dear Mr. Stransky,

On behalf of Hoover Institution fellows Mike Franc, Herb Lin and Amy Zegart, I would like to formally invite you to participate in Stanford's Congressional Cyber Boot Camp, held in Palo Alto, California on **August 14th - 17th, 2017.** The boot camp is a cross-institutional program created by Stanford's Hoover Institution, Center for International Security and Cooperation, and Freeman Spogli Institute for International Studies.

Designed to give select senior congressional staffers a deeper understanding of cybersecurity issues, the boot camp incorporates a broader network of experts from industry and academia to draw upon in the future. You will examine key technical, legal, economic, psychological, and organizational cyber policy challenges, participate in hands on simulations, taught by world renowned faculty, and engage in discussions with Silicon Valley leaders. We have also dedicated time for dialogue and questions that are of particular interest to you.

Confirmed speakers this year include: former Secretary of State Condoleezza Rice, former Ambassador to Russia Michael McFaul, former President of Estonia Toomas Hendrik Ilves, co-founder of Andreessen Horowitz, Marc Andreessen, plus many more from academia, tech, and the policy community. A field trip to Tesla's factory and headquarters is also slated on the agenda.

Stanford University will pay for reasonable travel expenses, including round-trip economy airfare, and ground transportation, business class lodging, and meals. The Boot Camp will not be financed in any part by a registered lobbyist or foreign agent, and will comply with all Congressional ethics rules. ***To participate in the Congressional Cyber Boot Camp, please submit the attached Ethics packet and notify Andrew Clark, afclark@stanford.edu, no later than July 14th.***

We are very much looking forward to your participation and welcoming you to sunny California this August.

Sincere regards,

Russell Wald

Russell C. Wald
Senior Manager for External Affairs
Hoover Institution, Stanford University

| Last Name | First Name | Title | Committee/Office | Chamber | Party | Gender |
|---|---|---|---|---|---|---|
| Arias | Jonathan | MLA | Senator Rubio | Senate | R | M |
| Burwell | Carter | Deputy Chief Counsel | Subcommittee on Constitution (Judiciary) | Senate | R | M |
| Carroll | Melika | Policy Advisor | Senator Schatz | Senate | D | F |
| Freedman | Brett | Counsel | SSCI | Senate | D | M |
| Kitchen | Klon | National Security Advisor | Sasse | Senate | R | M |
| Klein | Julie | PSM | HSGAC | Senate | D | F |
| Lazarus | Allison | PSM | SASC | Senate | R | F |
| Lips | Dan | PSM | HSGAC | Senate | R | M |
| McFeely | Tara | PSM | SSCI | Senate | R | F |
| Middleton | Bakari | Counsel | Booker | Senate | D | M |
| Nguyen | Minh | General Counsel | Senator McCain | Senate | R | F |
| Ravindra | Arjun | PSM | SSCI | Senate | R | M |
| Rossi | Nick | Staff Director | Commerce, Science, Transportation | Senate | R | M |
| Soifer | Halie | National Security Advisor | Senator Harris | Senate | D | F |
| Stransky | Michael | Policy Counsel | Republican Policy Committee | Senate | R | M |

THE STANFORD CYBER INITIATIVE | THE STUART FAMILY CONGRESSIONAL FELLOWSHIP PROGRAM

# CONGRESSIONAL CYBER BOOT CAMP

AUGUST 14-17, 2017

#STANFORDCYBER

HOOVER INSTITUTION | Center for International Security and Cooperation | Freeman Spogli Institute for International Studies

# SYLLABUS

## FACULTY CO-CHAIRS

Dr. Amy Zegart
Co-Director, Center for International Security and Cooperation (CISAC)
Davies Family Senior Fellow, Hoover Institution
Senior Fellow, Freeman Spogli Institute for International Studies (FSI)
Professor of Political Science (by courtesy), Stanford University

Dr. Herb Lin
Senior Research Scholar for Cyber Policy and Security, Center for International Security and Cooperation (CISAC)
Hank J. Holland Fellow in Cyber Policy and Security, Hoover Institution
Chief Scientist Emeritus, Computer Science and Telecommunications Board, National Academies

## COURSE DESCRIPTION

Modern nations are increasingly dependent on information and information technology for societal functions. Thus, ensuring the security of information and information technology —cybersecurity — against a broad spectrum of hackers, criminals, terrorists, and state actors is a critical task for the nation. Cybersecurity challenges are evolving at a rapid pace, and the cyber threat the nation faces today will be different from the one it faces tomorrow.

Cybersecurity is not solely a technical matter, although it is easy for policy analysts and others to get lost in the technical details. Improving cybersecurity is a multi-faceted enterprise that requires drawing on knowledge from computer science, economics, law, political science, psychology, and a host of other disciplines. Therefore, this Boot Camp draws upon the expertise of cyber scholars in academia as well as senior business and security professionals in Silicon Valley to provide perspectives on the many dimensions of this dynamic issue.

This Boot Camp will integrate multiple perspectives and disciplines to provide an understanding of the fundamentals of cybersecurity, the nature of cybersecurity threats, various approaches to addressing these threats, and the use of offensive cyber capabilities to advance national interests. The Stanford Cyber Boot Camp endeavors to give congressional staffers a conceptual framework to understand the threat environment of today and how it might evolve so that they are better able to anticipate and manage the problems of tomorrow.

## Day 1 (Monday, August 14): Cyber Attacks and Responses

**12:00 p.m. - 1:00 p.m.: Lunch & Keynote Address**

**RE-FRAMING THE "CYBERSECURITY " PROBLEM**

Faculty:

- **Sean Kanuck,** *Former National Intelligence Officer for Cyber Issues, Office of the Director of National Intelligence; CISAC affiliate*
- Introduction: Dr. Herb Lin, *Senior Research Scholar, CISAC; Hank J. Holland Fellow, Hoover Institution*

This session will overview the scope of the program (what we cover, what we don't, and why) and set the analytic stage for how we approach the rest of the course.

- **Scope**: The security implications and challenges of the nation's use of information technology. The course does not address topics such as consumer security, although many concepts covered are relevant.
- **Framing Theme #1**: Cybersecurity has different meanings and poses different challenges to different stakeholders. Approaching the problem posed requires understanding the perspectives of various actors, their interests, incentives, and organizational demands. Boot Camp sessions are designed to allow staffers to better understand the perspectives of different stakeholders and key players, including attackers and corporate executives.
- **Framing Theme #2**: The non-technical dimensions of cybersecurity (politics, organizational dynamics, economics, and psychology) are often far more important and less understood than the technical aspects. The Boot Camp pays explicit attention to these non-technical dimensions and how they intersect with technical challenges.
- **Framing Theme #3**: On the technical side, the course focuses on the underlying foundational principles of computing and communications technology (collectively, information technology) that drive the evolution of architectures, technologies, and vulnerabilities.
- **Framing Theme #4**: The Boot Camp explains the inherent dominance of offense over defense in cybersecurity and how this fact relates to the "cybersecurity problem."

**1:00 p.m. - 2:00 p.m.: Session 1**

**THINKING LIKE AN ATTACKER**

Faculty:

- **Dr. Earl Boebert,** *Senior Scientist, Sandia National Laboratories (Retired)*
- **Dr. Herb Lin,** *Senior Research Scholar, CISAC; Hank J. Holland Fellow, Hoover Institution*

Effectively combating any adversary requires understanding the ways in which that adversary thinks. Cybersecurity adversaries — from state agents seeking to disable military systems to hacktivists seeking to make a political point — share a security mindset: a predilection for examining the ways in which the security of a system can be circumvented or penetrated. Whereas good engineering is about how a system can be made to work, the security mindset involves thinking about how some aspect of a system can be made to fail. Understanding this mindset is the first step towards designing sound cybersecurity solutions.

Assignment: While in transit to the course location in Palo Alto, conduct a thought experiment for bringing an item prohibited by TSA regulations onto the airplane.

Learning Objectives: Why defense is more difficult than offense and what makes ongoing offense-defense competition inevitable.

**2:30 p.m. - 3:30 p.m.: Session 2**

**THREATS TO CYBERSECURITY**

Faculty:

- Carey Nachenberg, *Google X; Adjunct Assistant Professor of Computer Science, UCLA*

Cybersecurity compromises can take a variety of forms and occur for a variety of reasons. Session 2 examines these compromises and the vulnerabilities in information technology that allow them to happen, again reprising the theme of offensive dominance. This session will include a number of forensic case studies that illuminate the attack spectrum, key challenges, and trends.

Learning Objectives: Security-relevant principles of information technology; types of compromise; the inherent vulnerabilities of information technology; the hidden complexity of cyberspace; anatomy of security compromises; and the spectrum of threats to cybersecurity.

**3:45 p.m. - 4:15 p.m.: Keynote Remarks**

**THE VIEW FROM EUROPE**

Faculty:

- **Toomas Hendrik Ilves,** *Former President of Estonia; Distinguished Visiting Fellow at CISAC, Hoover, and FSI*
- *Introduction:* **Dr. Amy Zegart,** *Co-Director, CISAC; Davies Family Senior Fellow, Hoover Institution; Senior Fellow, FSI*

4:30 p.m. - 5:30 p.m.: Dinner & Session 3

## OFFENSIVE DIMENSIONS OF CYBERSECURITY

Faculty:

- **Jason Healey,** *Senior Research Scholar, Columbia University's School for International and Public Affairs; Hoover Visiting Fellow; CISAC Affiliate*
- **Dr. Herb Lin (Discussant),** *Senior Research Scholar, CISAC; Hank J. Holland Fellow, Hoover Institution*

Offensive activities — including those conducted for espionage and attack purposes —serve a variety of national goals. These goals include, but are not limited to, cyber defense. This discussion will summarize the required strategy, intelligence, and policy necessary for offensive cybersecurity.

Learning Objectives: The role of offensive operations in cyberspace for improving the nation's cybersecurity posture and for other purposes; the differences between attacks and exploitations and the importance of these differences; the scope and nature of U.S. command and control of offensive operations in cyberspace.

6:00 p.m. - 8:30 p.m.: Session 4

## SIMULATION: RESPONDING TO A CYBER CRISIS

Faculty:

- **Michael McNerney,** *Co-Founder and CEO of Efflux Systems; CISAC Affiliate*
- **Raj Shah,** *Managing Partner, Defense Innovation Unit Experimental (DIUx)*
- **Joe Sullivan,** *Chief Security Officer, Uber*
- **Ruby Zefo,** *Vice President of the Law & Policy Group and Chief Privacy & Security Counsel, Intel Corporation*
- **Dr. Amy Zegart (Chair),** *Co-Director, CISAC; Davies Family Senior Fellow, Hoover Institution; Senior Fellow, FSI*

In this exercise, congressional staffers assume the roles of business executives at a large tech company called Frizzle that has just discovered a major cyber breach. Early forensics indicate that a Frizzle employee opened a malicious PDF file containing a zero-day exploit. This vulnerability enabled the attackers to gain access to F-Net, the company's social networking platform, as well as the Frizzle email user accounts of Chechen activists and sympathizers. In addition, the malicious file may have spread through victims' emails to the Credit Luxe bank in Luxembourg, which processes more than two thirds of Frizzle's user payments. Frizzle's engineering/cybersecurity team, which is one of the best in the world, believes the attack came from Eastern Europe, though much remains unclear.

The CEO has called an emergency meeting of the Board of Directors to formulate a broad-based response to the cyber breach and has asked each of Frizzle's core teams – Engineering / Cybersecurity, Business Strategy, Legal, Public Policy, and Marketing / Communications – to develop and present actionable recommendations to the Board.

The Board of Directors is played by leading Silicon Valley security specialists, lawyers, and entrepreneurs with extensive experience in cybersecurity and business. Board Members attend team breakout sessions and in the "full board meeting" question and discuss each team's recommendations. The simulation concludes with a debrief session where staffers reflect on the simulation and Board Members share insights from their actual experiences confronting cyber challenges.

Learning Objectives: To walk in the shoes of business leaders confronting the early hours and critical decisions of a cyber crisis. Who exactly is hurt or could be hurt by the breach? How could the breach impact Frizzle's business in different markets and its brand reputation? Who are the key stakeholders and how might they react? What actions should Frizzle take and what are the tradeoffs? Should the company "hack back" or publicize the breach to its users, its European bank, its competitors? Work with U.S. government agencies? How do Frizzle's mission and corporate culture guide its response? These are some of the questions staffers will consider.

## Day 2 (Tuesday, August 15): Deep Dive: Technical & Nontechnical Aspects of Cyber

**8:30 a.m. - 10:00 a.m.: Breakfast and Keynote Conversation**

**KEYNOTE** Industry and Policy Challenges in Cybersecurity

Faculty:

- **Dr. Condoleezza Rice,** *Thomas and Barbara Stephenson Senior Fellow, Hoover Institution; Denning Professor, Stanford Graduate School of Business; former U.S. Secretary of State and National Security Advisor*
- **Marc Andreessen,** *Co-Founder and General Partner of Andreessen Horowitz*
- *Introduction:* **Dr. Amy Zegart,** *Co-Director, CISAC; Davies Family Senior Fellow, Hoover Institution; Senior Fellow, FSI*

**10:15 a.m. - 11:15 a.m.: Session 5**

**FUNDAMENTAL PRINCIPLES OF CYBERSECURITY**

Faculty:

- **Dr. Irving Lachow, Portfolio Manager, International Cyber, MITRE;** *Visiting Fellow Hoover Institution; Affiliate, CISAC*
- **Dr. John Villasenor,** *Professor of Electrical Engineering, Public Policy, and Management, UCLA; Visiting Professor of Law, UCLA; Visiting Fellow, Hoove Institution; Affiliate, CISAC*

Although cybersecurity can be a deeply technical subject, especially in how cybersecurity solutions are implemented, a few fundamental principles underlie most solutions. This session takes a deep dive into the fundamental principles of improving cybersecurity and how they fit together. These include reducing reliance on information technology, detecting cybersecurity compromises, and blocking and limiting the impact of compromise. Additional topics include authentication, access control, forensics, recovery, containment, resilience, and active defense.

Learning Objectives: The value of these fundamental principles of cybersecurity and how they can be used collectively to improve security.

**11:45 a.m. - 12:45 p.m.: Lunch & Session 6**

**ECONOMIC & ORGANIZATIONAL DIMENSIONS OF CYBERSECURITY**

Faculty:

- **Dr. Dave Clark,** *Senior Research Scientist at the MIT Computer Science and Artificial Intelligence Laboratory*
- **Dr. Tyler Moore,** *Tandy Assistant Professor of Cyber Security and Information Assurance, University of Tulsa*

Known cybersecurity measures are often fully adopted due to a variety of economic and organizational factors. These factors are non-technical in nature and often underappreciated by technical and policy communities. Economics describe the incentives that apply to cyber defenders and adversaries, including the nature of cybersecurity market failures and the ability to handle collective action problems. An organizational perspective addresses the structural necessities and importance of organizational culture to cybersecurity. This session examines how these factors often discourage the adoption of sound security practices.

Learning Objectives: The importance of economic and organizational factors of cybersecurity and why they are often overlooked in efforts to improve cybersecurity; how government action might help to address non-technical factors that diminish the nation's cybersecurity posture.

**1:30 p.m. - 2:30 p.m.: Session 7**

**DOMESTIC LAW AND INTERNATIONAL LEGAL DIMENSIONS OF CYBER SECURITY**

Faculty:

- **Prof. Matthew Waxman,** *Liviu Librescu Professor of Law, Faculty Chair Roger Hertog Program on Law and National Security, Columbia University*
- **Prof. Robert Chesney,** *Associate Dean and Charles I. Francis Professor, University of Texas School of Law; Director, Robert S. Strauss Center for International Security and Law*

Technological change has far outpaced changes in law and will almost certainly continue to do so in the future. This lag consequentially challenges Congress to craft legislation appropriate for future technology. Furthermore, nations have cooperative and competitive (and sometimes adversarial) interests that play out in cyberspace. Internet communication does not inherently respect national borders, giving an international dimension to every cybersecurity challenge.
Learning Objectives: For domestic law, the implicit technological assumptions of existing cybersecurity laws; what problems arise in applying existing law to technological circumstances not contemplated at the time of initial passage.

For international dimensions, various legal regimes of potential relevance, including the law of war, human rights law, trade and intellectual property law; proposals for Internet governance; and different non-governmental organizations that affect the design and operation of the Internet.

**2:30 p.m. - 3:00 p.m.**

**DEBRIEF from previous day**

Faculty:

- **Dr. Herb Lin,** *Senior Research Scholar, CISAC; Hank J. Holland Fellow, Hoover Institution*
- **Dr. Amy Zegart,** *Co-Director, CISAC; Davies Family Senior Fellow, Hoover Institution; Senior Fellow, FSI*

**3:00 p.m. - 4:00 p.m.**

HOOVER ARCHIVES OR STANFORD WALKING TOUR

- **Archive Tour: Jean Cannon,** *Assistant Archivist - Communications & Outreach*
- **Walking tour: Rachel Hirshman,** *Stanford Student*

**5:30 p.m. - 8:30 p.m.: Reception & Dinner**

KEYNOTE Cyber Challenges From the C-Suite to the Kremlin

Faculty:

- **Dr. Michael McFaul,** *Director and Senior Fellow, FSI; Peter and Helen Bing Senior Fellow, Hoover Institution, Professor of Political Science, Stanford University; former U.S. Ambassador to the Russian Federation*
- **Joel Peterson,** *Chairman, JetBlue Airways; Robert L. Joss Adjunct Professor of Management, Stanford Graduate School of Business; Chairman, Hoover Institution Board of Overseers*
- Introduction: **Mike Franc,** *Director, Hoover DC office*
- Moderator: **Dr. Amy Zegart,** *Co-Director, CISAC; Davies Family Senior Fellow, Hoover Institution; Senior Fellow, FSI*

## Day 3 (Wednesday, August 16): Civil Liberties, Corporate Interests, and Security

**7:45 a.m. - 8:30 a.m.: Breakfast**

**DEBRIEF from previous day**

Faculty:

- **Dr. Herb Lin,** *Senior Research Scholar, CISAC; Hank J. Holland Fellow, Hoover Institution*
- **Dr. Amy Zegart,** *Co-Director, CISAC; Davies Family Senior Fellow, Hoover Institution; Senior Fellow, FSI*

**8:30 a.m. - 9:30 a.m.: Session 8**

**CYBERSECURITY AND CIVIL LIBERTIES**

Faculty:

- **Anne Neuberger,** *Deputy Director of Operations, National Security Agency*
- **Jennifer Granick,** *Director of Civil Liberties, Stanford Center for Internet and Society; Affiliate, CISAC; Former Civil Liberties Director, Electronic Frontier Foundation*

Measures intended to support cybersecurity can also threaten certain civil liberties. What cybersecurity means depends in part on whose security is at risk. For some, a threat to civil liberties resulting from greater use of information technology might be interpreted as a cybersecurity threat. Session 8 focuses on this push and pull between security and civil liberties in cyberspace.

Learning Objectives: Different perspectives at the nexus of civil liberties and cybersecurity; how, when, and to what extent, preservation of civil liberties and cybersecurity trade off against one another. Topics to be discussed include privacy, anonymity, and free speech.

**9:30 a.m. - 10:30 a.m.: Session 9**

**INDUSTRY PERSPECTIVES ON CYBERSECURITY**

Faculty:

- **Dr. Sameer Bhalotra (Chair),** *Co-Founder and CEO, StackRox; Senior Associate of the Strategic Technologies Program, CSIS; Affiliate, CISAC; former Senior Director for Cybersecurity, National Security Council*
- **Bandel Carano,** *Managing Partner, Oak Investment Partners*
- **Rick Howard,** *Chief Security Officer, Palo Alto Networks*
- **Claire Hughes Johnson,** *COO, Stripe*
- **Matt Miller,** *Partner, Sequoia Capital*

Market forces have a critical role in enhancing or weakening cybersecurity. Session 9 examines how such forces play out at the level of the individual firm and incorporate the views and concerns of the business community. Silicon Valley senior executives and engineers will give their "cyber-ground truths" about the security problems facing the private sector.

Learning Objectives: Various private sector perspectives from technology firms that support innovative efforts for providing IT-based products and services with attention to cybersecurity.

**11:00 p.m. - 11:45 p.m.: Session 10**

**WHITE HOUSE PERSPECTIVES**

Faculty:

- **Andy Grotto,** *CISAC Perry Fellow; Hoover Research Fellow; Affiliate, CISAC; Former Senior Director for Cybersecurity Policy, National Security Council*

**12:00 p.m. - 1:30 p.m.: Lunch Keynote**

**DRIVERLESS CARS & PLANE HACKING: SECURITY VULNERABLITIES, CAUSES, AND CHALLENGES**

Faculty:

- **Dr. Stefan Savage,** *Professor of Computer Science and Engineering, UCSD; Director, Center for Network Systems (CNS); Co-Director, Center for Evidence-based Security Research (CESR)*

Modern automobiles are no longer mere mechanical devices; they are pervasively monitored and controlled by dozens of digital computers coordinated via internal vehicular networks. While this transformation has driven major advancements in efficiency and safety, it has also introduced a range of new potential risks. In 2010, University of California, San Diego and the University of Washington demonstrated the ability to remotely control a popular passenger vehicle with no prior physical access. Recent demonstrations have validated that similar issues exist in other vehicles as well.

Learning Objectives: The nature of automotive security vulnerabilities, the underlying causes, and the challenges (both technical and non-technical) in securing the automotive platform.

**2:30 p.m. - 4:30 p.m.**

## TESLA FACTORY VISIT

Technology companies are leading innovation and changing the world. Tesla was founded in Silicon Valley in 2003 with the goal to manufacture zero-emission electric cars and has experienced goal exponential growth in this field. Today Tesla has expanded its mission to specialize in batteries and sustainable solar energy. While this transformation has driven major advancements in efficiency, it has also introduced a range of new potential cyber risks.

Learning Objectives: By engaging directly with senior engineers at the Tesla Factory, Congressional staffers will be exposed to the complexities of a tech firm at the center of innovation.

**Tesla Factory**
**45500 Fremont Blvd, Fremont, CA 94538**

**6:30 p.m. - 8:30 p.m.**

## DINNER: Debrief & Next Steps

**Coupa Café – Stanford Golf Course**
**198 Junipero Serra Blvd, Stanford, CA, 94305**